

Filter 基本配置指南

（适用）AT-8600/8700XL/Rapier i/8800 系列交换机

ATC-TS1014

V1.0

2005-12-1



1. 概述

本文介绍如何配置使用安奈特设备中的各种 Filter（过滤器）。

2. 实施需求

正确实现该功能有以下实施需求：

- AT-8600/8700XL/Rapier i/8800 系列交换机

3. Filter 介绍

安奈特系列交换机可以配置多种 Filter，总结有如下几种：

- SWITCH FILTER；
- SWITCH HWFILTER；
- SWITCH L3FILTER；
- IP TRAFFIC FILTER；
- IP POLICY FILTER；
- IP PRIORITY FILTER；
- IP ROUTING FILTER。

从它们的名字可以看出，这些 Filter 实际上可以分为两大类，即 Switch 类和 IP 类。这两类 Filter 由于运行方式不同，导致运行结果也不相同。Switch 类的 Filter 由交换机交换芯片执行，硬件实现，运行快，对交换机性能没有影响，但由于交换芯片限制，不够灵活，实现功能也有限。IP 类 Filter 由交换机 CPU 执行，软件实现，可以配合其它特性实现多种功能，但对性能会有影响。

从图 1 中可以看到各种 Filter 之间的关系及分类。



图 1

Filter
Switch
L2 Filter
Hardware Packet Filter
SWITCH FILTER
SWITCH HWFILTER
SWITCH L3FILTER
IP
IP TRAFFIC FILTER
IP POLICY FILTER
IP PRIORITY FILTER
IP ROUTING FILTER

SWITCH HWFILTER 和 SWITCH L3FILTER 是 Switch 类 Filter 中 Hardware Packet Filter 的两中不同的表现形式。虽然它们在交换机中配置有完全不同的命令形式，但实现的方式效果是完全相同的。

全部的 IP Filter 使用都使用 ADD IP FILTER 命令来配置，依据不同 Filter ID 范围来区分不同功能的 Filter。0 到 99 被用作 IP TRAFFIC FILTER ；100 到 199 被用作 IP POLICY FILTER；200 到 299 被用作 IP PRIORITY FILTER；300 到 399 被用作 IP ROUTING FILTER。

常用于流量过滤的是 0 到 99 的 IP TRAFFIC FILTER，而 IP POLICY FILTER 用于策略路由，IP PRIORITY FILTER 用于优先级路由，IP ROUTING FILTER 用于路由信息过滤。



4. 实例

4.1 SWITCH FILTER

SWITCH FILTER 主要用于 MAC 地址和交换机端口的静态绑定。交换机的一个端口最多可以绑定 256 条 MAC 地址。静态的 SWITCH FILTER 可以将一个 MAC 地址和 VLAN 以及端口关联到一起，当交换机接收到一个目的地址和 VLAN 标识符和 SWITCH FILTER 条目匹配的帧后，可以依据该条目定义的行为转发到指定端口或者丢弃。

实例 1：

转发目的 MAC 地址是 00-00-cd-12-34-56 在交换机端口 3 的数据帧。

```
ADD SWITCH FILTER DESTADDRESS=00-00-cd-12-34-56 ACTION=FORWARD PORT=3
```

丢弃所有目的 MAC 地址是 00-00-cd-12-34-56 在 VLAN4 中端口 4 的数据帧。

```
ADD SWITCH FILTER DESTADDRESS=00-00-cd-12-34-56 PORT=4 ACTION=DISCARD
VLAN=4
```

4.2 Switch Hardware Packet Filter

Switch Hardware Packet Filter 主要有两种：SWITCH HWFILTER 和 SWITCH L3FILTER。

两种 Filter 实现效果完全相同。SWITCH HWFILTER 基于 Packet Classifier 实现；SWITCH L3FILTER 基于自有的 L3 match 条目实现。两种不能同时使用。

由于 Internet Group Management Protocol (IGMP) snooping 也使用 Hardware Packet Filter，启用 IGMP snooping 会影响 filter 使用的数量。因此可能在使用这两种 Hardware Packet Filter 时，需要禁用 IGMP snooping。



Switch Hardware Packet Filter 可以实现访问控制列表功能，用于过滤流量，这一点与 IP TRAFFIC FILTER 非常相似。由于 Switch Hardware Packet Filter 是硬件实现，对交换机性能没有影响，因此在需要过滤流量时，应尽量使用 Switch Hardware Packet Filter。

实例 2：

限制 192.168.10.0/24 子网的 WEB 服务，只允许 192.168.20.0/24 子网访问。其余经过交换机的流量不限制。

定义分类器匹配所有到 192.168.10.0/24 子网的 WEB 访问流量。

```
CREATE CLASSIFIER=1 IPDADDR=192.168.10.0/24 TCPDPORT=80
```

创建一个 SWITCH HWFILTER 拒绝所有的上述流量。

```
ADD SWITCH HWFILTER CLASSIFIER=1 ACTION=DENY
```

定义分类器匹配所有 192.168.20.0/24 子网到 192.168.10.0/24 子网的 WEB 访问流量。

```
CREATE CLASSIFIER=2 IPDADDR=192.168.10.0/24 IPSADDR=192.168.20.0/24
TCPDPORT=80
```

创建一个 SWITCH HWFILTER 允许的上述流量。

```
ADD SWITCH HWFILTER CLASSIFIER=2 ACTION=NODROP
```

注意：

1、一个分类器对应一个 SWITCH HWFILTER；

2、多个 SWITCH HWFILTER 是由上至下以线性次序进行匹配的；

3、如果没有匹配，没有定义未匹配行为，那么数据包将会被传输；



4、"ACTION=DENY"并不是匹配后就马上丢弃，而是在所有的 SWITCH HWFILTER 执行完后，没有匹配才丢弃。

5、"NODROP"参数，是指匹配流量如果被前面规则标识拒绝，则不丢弃，正常转发。请特别注意，该参数只有 Rapier i 系列交换机才有。

6、对应 Rapier i 系列交换机，如果使用分类器中的进端口（ingress port）和出端口（egress port）作为匹配条件，使用该分类器的 SWITCH HWFILTER 所有的 ACTION 参数都是有效的。但是，不会匹配该分类器中的其它参数。

实例 3：

允许所有到 TCP 目的端口 25 和 80，UDP 目的端口 5151 的流量，但拒绝所有其它的流量。

定义分类器匹配所有到 tcp 目的端口 80 的流量。

```
CREATE CLASSIFIER=1 TCPDPORT=80
```

创建一个 SWITCH HWFILTER，所有的上述流量将被转发，所有不匹配流量将被拒绝。

```
ADD SWITCH HWFILTER CLASSIFIER=1 ACTION=FORWARD NOMATCHACTION=DENY
```

定义分类器匹配所有到 tcp 目的端口 25 的流量。

```
CREATE CLASSIFIER=2 TCPDPORT=25
```

创建一个 SWITCH HWFILTER，所有的上述流量将被转发，所有不匹配流量将被拒绝。

```
ADD SWITCH HWFILTER CLASSIFIER=2 ACTION=FORWARD NOMATCHACTION=DENY
```

定义分类器匹配所有到 udp 目的端口 5151 的流量。

```
CREATE CLASSIFIER=3 UDPDPORT=5151
```

创建一个 SWITCH HWFILTER，所有的上述流量将被转发，所有不匹配流量将被拒绝。



```
ADD SWITCH HWFILTER CLASSIFIER=3 ACTION=FORWARD NOMATCHACTION=DENY
```

4.3 IP TRAFFIC FILTER

ID 0 到 99 的 IP FILTER 用于流量过滤。

用于流量过滤的 IP TRAFFIC FILTER 是应用于接口的，而用于流量过滤的 Hardware Packet Filter 是应用于交换机全局的。当有 IP 流量到达使用了 IP FILTER 的接口时，将依据匹配模式决定是否转发。

IP TRAFFIC FILTER 也时以线性次序进行匹配执行的，遇到第一条匹配的条目时将停止匹配。因此，各条目的先后顺序特别重要。为了提高效率，最常使用的条目应该放到最上面。在没有匹配的条目时，缺省将拒绝该流量。

注意：一个接口只能应用一条 IP TRAFFIC FILTER。

实例 4：

图 2

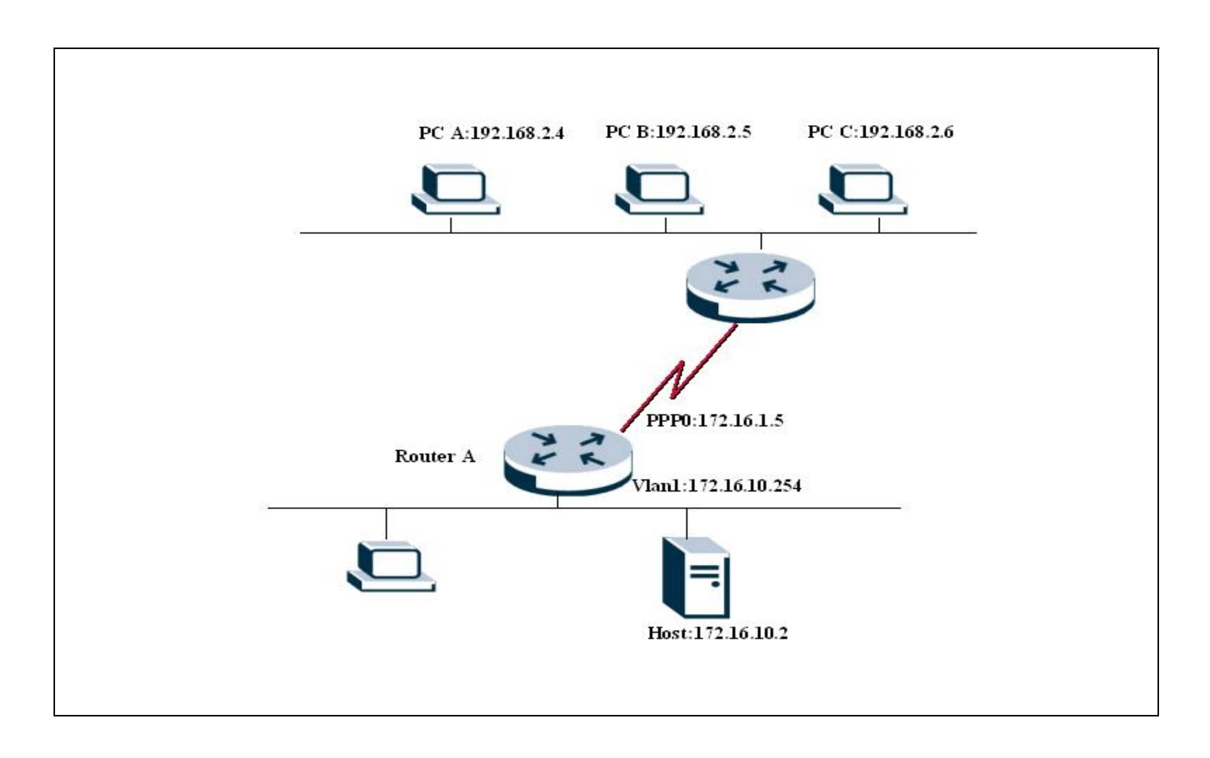


图 2 中，定义 IP TRAFFIC FILTER，实现下列规则：



- 允许 PC A 到 Host 的 telnet 访问；
- 允许 PC B 到 Host 的 telnet 和 ftp 访问；
- 允许 PC C 到 Host 的 ftp 访问；
- 拒绝其它所有的访问，包括从 Host 网段到 PC 网段的访问。

在 Router A 上做如下配置：

定义 filter 1 应用于 PPP 0 接口，用于限制 PC 网段到 Host 网段的访问。

允许 PC A 到 Host 的 telnet 访问

```
ENABLE IP

ADD IP FILT=1 SO=192.168.2.4 SM=255.255.255.255 DEST=172.16.10.2 DM=255.255.255.255 DPORT=TELNET  PROT=TCP SESS=ANY AC=INCLUDE
```

允许 PC B 到 Host 的 telnet 和 ftp 访问

```
ADD IP FILT=1 SO=192.168.2.5 SM=255.255.255.255 DEST=172.16.10.2 DM=255.255.255.255 DP=FTPDATA PROT=TCP SESS=ESTA AC=INCL

ADD IP FILT=1 SO=192.168.2.5 SM=255.255.255.255 DEST=172.16.10.2 DM=255.255.255.255 DP=FTP PROT=TCP SESS=ANY AC=INCL

ADD IP FILT=1 SO=192.168.2.5 SM=255.255.255.255 DEST=172.16.10.2 DM=255.255.255.255 DP=TELNET PROT=TCP SESS=ANY AC=INCL
```

允许 PC C 到 Host 的 ftp 访问

```
ADD IP FILT=1 SO=192.168.2.6 SM=255.255.255.255 DEST=172.16.10.2 DM=255.255.255.255 DP=FTP PROT=TCP SESS=ESTA AC=INCL

ADD IP FILT=1 SO=192.168.2.6 SM=255.255.255.255 DEST=172.16.10.2 DM=255.255.255.255 DP=FTPDATA PROT=TCP SESS=ESTA AC=INCL
```



定义 filter 2 应用于 Vlan 1 接口，仅允许 Host 到 PC 网段的应答流量通过。

允许 Host 到 PC A 的 telnet 应答流量

ADD IP FILT=2 SO=172.16.10.2 SM=255.255.255.255 SP=TELNET DEST=192.168.2.4 DM=255.255.255.255 PROT=TCP SESS=ESTA AC=INCL

允许 Host 到 PC B 的 telnet 和 ftp 应答流量

ADD IP FILT=2 SO=172.16.10.2 SM=255.255.255.255 SP=TELNET DEST=192.168.2.5 DM=255.255.255.255 PROT=TCP SESS=ESTA AC=INCL

ADD IP FILT=2 SO=172.16.10.2 SM=255.255.255.255 SP=FTPDATA DEST=192.168.2.5 DM=255.255.255.255 PROT=TCP SESS=ANY AC=INCL

ADD IP FILT=2 SO=172.16.10.2 SM=255.255.255.255 SP=FTP DEST=192.168.2.5 DM=255.255.255.255 PROT=TCP SESS=ESTA AC=INCL

允许 Host 到 PC C 的 ftp 应答流量

ADD IP FILT=2 SO=172.16.10.2 SM=255.255.255.255 SP=FTPDATA DEST=192.168.2.6 DM=255.255.255.255 PROT=TCP SESS=ANY AC=INCL

ADD IP FILT=2 SO=172.16.10.2 SM=255.255.255.255 SP=FTP DEST=192.168.2.6 DM=255.255.255.255 PROT=TCP SESS=ESTA AC=INCL

应用 Filter 到接口。

CREATE PPP=0 OVER=SYN0

ADD IP INT=vlan1 IP=172.16.10.54 MASK=255.255.255.0 FILT=2

ADD IP INT=ppp0 IP=172.16.1.5 MASK=255.255.255.0 FILT=1



关于安奈特（Allied Telesyn）

安奈特（Allied Telesyn）作为全球知名的网络产品和解决方案供应商，拥有遍布世界各地的 200 多个公司和分支机构。自 1987 年成立以来，安奈特专注于为用户提供高安全性、高可靠性、易于管理、易于维护、易于升级的网络系统解决方案。

公司在世界各地设立了十余个强大的研发机构，时刻跟踪最新的科技进步成果，了解客户的需求，及时推出性能优异、契合需求的全系列产品，包括从接入、汇聚、核心到传输的以太网交换机、路由器、电信综合接入平台、介质转换器、VoIP 产品以及高性能操作系统和网络管理平台。安奈特自成立以来一直保持稳定的高增长态势，成为全球发展最快的高科技公司之一。

1999 年，安奈特在北京成立了安奈特（中国）网络有限公司。2002 年在东莞设立了全资工厂，还在全国各大区增设了办事处，并进一步完善了技术服务体系、认证培训体系和渠道运营体系，以便更好地为中国客户服务，满足不同行业和领域客户需求。

欲知详情，请致电安奈特公司及其各分支机构，或访问 www.alliedtelesyn.com.cn

北京（中国总部及北方区办事处）
负责地区：东北三省、北京、内蒙古、天津、河北、山西、山东、河南、陕西、甘肃、青海
地址：北京市朝阳区朝外大街 16 号中国人寿大厦 1007-1009 室
邮编：100020　　电话：(010)85252299 传真：(010)85252298
上海（华东区办事处）
负责地区：上海、江苏、安徽、浙江、湖北、江西
地址：上海市南京西路 1168 号中信泰富广场 3405 室
邮编：200041　　电话：(021)52984245/46/47　　传真：(021)52984239
广州（华南区办事处）
负责地区：广东、广西、海南、福建、湖南
地址：广州市天河北路 233 号中信广场 1102 室
邮编：510613　　电话：(020)38911922 传真：(020)38911303
成都（华西区办事处）
负责地区：四川、重庆、贵州、云南、西藏、新疆、宁夏
地址：四川省成都市顺城大街 308 号冠城广场 19 层 H 座
邮编：610017　　电话：(028)86527190 传真：(028)86527193
香港（安奈特北亚区总部）
负责地区：香港、澳门、台湾、韩国
地址：香港官塘官塘道 418 号创纪之城 5 期东亚银行中心 18 楼 1812-1816 室
电话：(00852)22636566　传真：(00852) 27568130 / 23180720
USA Headquarters:
19800 North Creek Pkwy, Suite 200, Bothell, WA 98011, USA
Tel: 800.424.4284 Fax: 425.481.3895
European Headquarters: Via Motta 24, 6830 Chiasso, Switzerland
(Corporate) Tel: (+41) 91 697.69.00 Fax: (+41) 91 697.69.11
(European Sales) Tel: (+39) 02 414.112.1 Fax: (+39) 02 414.112.61